UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,914	12/10/1999	GERMANO CARONNI	06502.0289	8208

58328 7590 02/03/2009

SUN MICROSYSTEMS
C/O SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
02/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/457,914	CARONNI ET AL.	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-11,22,24-31,33-37,39 and 41-45* is/are pending in the application.

4a) Of the above claim(s) *4,6,12,21,23,32,38,40 and 46-48* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-11,22,24-31,33-37,39 and 41-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-45 are pending.

Claims 4, 6, 12, 21, 23, 32, 38, 40, and 46-48 are cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/24/2008 has been entered.

Response to Arguments

3. Applicant's arguments filed 11/24/08 have been fully considered but they are not persuasive.

In response to applicant's argument that Mattaway fails to teach or suggest determining if the first and second process belong to a channel and accepting the transmitted packet if the processes belongs to a channel. Mattaway is combined with Shuen to teach the obviousness of transmitting a packet from the first process to the second process through the open socket without passing through the administrative machine. Thus, Shuen suggests the new limitation of belong to a channel. Shuen discloses networks may include lines connecting to various nodes and an

access point includes a transmitter and receiver operating at some electromagnetic frequency. Corresponding to an access point may be an access point card (col.13, lines 49-64 and col.14, lines 15-55). A channel is necessary to be established for any communication or transmission to occur. Thus, the access point establishes a channel in order to allow communication or connection amongst nodes, systems, or networks. Hence, the frequency or link is also interpreted and given as a channel that the access point interconnects the card and allows connection to devices which suggests a channel is determined if the access point has been determined corresponding to the card that permits communication amongst the network (col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shuen (US 5,572,528), in view of Mattaway, et al. (US 6,226,678).

As per claims 1, 18, and 35:

Shuen, et al. teaches a method executed in a data processing system for providing communication access between a first process associated with a first node and a second process associated with a second node **(col.18, lines 14-43)**, the method comprising:

sending a request from the first node to an administrative machine **(col.23, lines 36-47 and col.25, lines 14-35)** to verify a first node identification **(col.7, lines 54-57 and col.16, lines 41-55 and col.22, lines 62-65)** associated with the first process; **(col.8, lines 19-27 and col.9, lines 32-36 and col.23, lines 12-22)**

in response to the request, receiving security context information at the first node from the administrative machine **(col.23, lines 60-65 and col.25, lines 14-35)**, the security context information comprising a virtual address for the first node; **(col.9, lines 11-15 and col.13, lines 7-8 and 42-48)**

appending the security context information for the first process in a process table **(col.12, lines 64-67 and col.13, lines 1-13)**, the process table listing a first process identifier associated with the first process executing in memory; **(col.18, lines 45-55 and col.25, lines 50-54)**

opening a socket between the first process and the second process; and **(col.23, lines 26-30)**

transmitting a packet from the first process to the second process through the open socket **(col.22, lines 13-15 and col.23, lines 8-24)** *[without passing through the administrative machine]*, the packet comprising the security context information for the first process in the process table. **(col.15, lines 10-35 and col.18, lines 50-65 and col.19, lines 13-15)**

determining if the first and second process belong to a channel; and **(col.13, lines 49-64 and col.14, lines 40-55)**

accepting the transmitted packet when the first and second process belong to the channel.

(col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53)

Shuen discloses networks may include lines connecting to various nodes and an access point includes a transmitter and receiver operating at some electromagnetic frequency. Corresponding to an access point may be an access point card (col.13, lines 49-64 and col.14, lines 15-55). The access point establishes a channel in order to allow communication or connection amongst nodes, systems, or networks. Thus, the frequency or link is also interpreted and given as a channel that the access point interconnects the card and allows connection to devices which suggests a channel is determined if the access point has been determined corresponding to the card which permits communication amongst the network (col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53).

The claimed process associated with a node can broadly be given as a function for communication, routing, connection, session, etc. which usually includes packets or messages of information regarding the communication (col.12, lines 41-50 and col.21, lines 15-26). Shuen discloses a node is also referred as a host or mobile host (col.13, lines 50-52) and the claimed administrative machine as a home router. Shuen explains the request (col.23, lines 36-47 and col.25, lines 14-35) to verify a first node identification associated with the first process involves the mobile host exchanges information with the home router to respond to the mobile host. The exchanged information is a local address comprising local network number and a local node number that corresponds to the local network number that may be obtained from the router which is valid (col.16, lines 41-55 and col.22, lines 62-65). The constant address corresponding to a virtual network and virtual node number created by the home router and uniquely identifying the

mobile host throughout a session (col.7, lines 54-57). This information reads on the claimed first node identification associated with the first process. The constant address is the claimed virtual address where a constant address identifies a mobile host. Since the constant address is referenced to a virtual network number, it is called a virtual address (col.9, lines 11-15 and col.13, lines 7-8 and 42-48). The virtual network number and virtual node number are included in the virtual address (col.16, lines 62-67). The claimed without passing through the administrative machine obviously suggests the mobile host directly communicating with another node and not to the router (col.19, lines 13-15). Shuen discloses a mobile host may use its constant address to initiate sessions with a correspondent host (col.18, lines 60-65 and col.22, lines 13-15) and a sequenced packet exchange is an exchange of information according to a protocol by which two nodes may communicate across the network (col.30 , lines 24-34). Shuen obviously suggests a first process transmit a packet to the second process through the open socket. However, Shuen did not clearly explain transmitting a packet from the first process to the second process through the open socket without passing through the administrative machine.

Mattaway discloses the first processing unit 12 is the claimed first node and the second processing unit as the claimed second node. The claimed administrative machine can broadly be given as a server. Whether it is the connection server or mail server (col.8, line 65 – col.9, line 13 and col.12, lines 21-24), Mattaway's invention is for the first processing unit to establish direct communication links to the second processing unit without interacting or going through any server (col.9, lines 52-57 and col.26, lines 18-25). Mattaway discloses uses the server (col.7, lines 9-20) to verify a first node identification associated with the first process (col.3, lines 7-10 and col.18, lines 21-25). Mattaway discloses receiving security context information at the first node from the

administrative machine, the security context information comprising a virtual address for the first node (col.7, lines 24-28 and col.18, lines 33-36) and appending the security context information for the first process in a process table (col.18, lines 21-36 and col.20, lines 15-23). A process table obviously is for comparison and matching purposes to verify or validate the received data in the packet (col.18, lines 30-36). The packet comprising the security context information for the first process in the process table (col.22, lines 21-26). Mattaway discloses point-to-point Internet communication of transmitting a packet from the first process to the second process (col.8, lines 28-29) through the open socket without processing by a server (col.8, line 65 – col.9, line 13). The only purpose is for directory and information related services (col.12, lines 36-41 and col.17, lines 17-18). Thus, Mattaway suggests direct communication link between the first process and the second process without passing through a server (col.9, lines 52-57 and col.26, lines 18-25).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Shuen to teach transmitting a packet from the first process to the second process through the open socket (Mattaway on col.8, lines 28-29) without passing through the administrative machine (Mattaway on col.8, line 65 – col.9, line 13) because using a server (administrative machine) is for directory and information related services only and to verify a node so that the node can directly communicate with another node (Mattaway on col.12, lines 15-16 and 36-41 and col.26, lines 18-25).

As per claims 2, 19, and 36: See Shuen on col.21, lines 54-58 and col.23, lines 6-28; discusses modifying a socket structure so as to accept the security context information.

As per claims 3, 20, and 37: See Shuen on col.16, lines 41-55 and col.23, lines 5-30; discusses receiving the packet at the second process through the socket (Mattaway on col.22,

lines 48-50); verifying the security context information received in the packet; and permitting use of the packet if the security context information is verified (Mattaway on col.2, lines 46-50).

As per claims 5, 22, and 39: See Shuen on col.18, lines 52-55 and Mattaway on col.18, lines 21-36; discusses comparing the security context information in the received packet and security context information in another process table.

As per claims 7, 24, and 41: See Shuen on col.10, lines 35-37 and col.22, lines 50-52 and on Mattaway on col.12, lines 36-38; discusses determining whether the first and second process belong to two different linked channels; and permitting use of the packet when the different channels are linked.

As per claims 8, 25, and 42: See Shuen on col.18, lines 60-65 and col.22, lines 13-15 on Mattaway on col.12, lines36-38; discusses determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claims 9, 26 and 43: See Mattaway on col.3, lines 7-12 and col.16, lines 13-15; discusses permitting use of the packet includes decrypting the packet on a node and authenticating a sender associated with the first process on the node.

As per claims 10 and 27: See Shuen on col.8, lines 20-22 and col.22, lines 5-14; discusses obtaining the security context information from a third process, the security context information comprising a virtual address and a node identification.

As per claims 11, 28 and 45: See Shuen on col.17, lines 13-24 and col.23, lines 5-30; discusses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

As per claim 13: See Shuen on col.16, lines 41-55 and col.18, lines 46-49; discusses receiving a key that corresponds to the first node identification from the server.

As per claim 14: See Shuen on col.15, lines 10-35 and Mattaway on col.26, lines 46-50; discusses encrypting a packet transmitted by the first process using the key; and encapsulating the encrypted packet with a header that comprises the first node identification.

As per claim 15: See Shuen on col.16, lines 41-55 and col.18, lines 46-49 and col.22, lines 10-14 and 62-65; discusses a method of claim 1, further comprising: sending a second request from the second node to the server to verify node identification (Mattaway on col.2, lines 46-50); receiving additional security context information comprises from the server, wherein the additional security context information includes a second virtual address for the second node; creating the second process; and appending the security context information for the second process in the process table associated with the second process (Mattaway on col.18, lines 21-36).

As per claims 16 and 33:

Shuen teaches a method executed in a data processing system for providing secure communications between a first process associated with a first node and a second process associated with a second node **(col.18, lines 14-43)**, comprising:

obtaining node identification comprising a virtual address from an administrative machine; **(col.7, lines 54-57 and col.16, lines 41-55 and col.22, lines 62-65)**

including the node identification in a field corresponding to the first process **(col.8, lines 19-27 and col.23, lines 12-22)** in a process table **(col.12, lines 64-67 and col.13, lines 1-13)**, the process table listing a first process identifier associated with the first process executing in memory; **(col.18, lines 45-55 and col.25, lines 50-54)**

transmitting a datagram that contains the node identification the first process to a socket; and **(col.22, lines 13-15 and col.23, lines 8-30)**

receiving the datagram at the second process that contains the node identification and a second virtual address, *[without passing through the administrative machine]* **(col.9, lines 11-15 and col.13, lines 7-8 and 42-48)**

determining if the first and second process belong to a channel; and **(col.13, lines 49-64 and col.14, lines 40-55)**

accepting the transmitted packet when the first and second process belong to the channel. **(col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53)**

Shuen discloses networks may include lines connecting to various nodes and an access point includes a transmitter and receiver operating at some electromagnetic frequency. Corresponding to an access point may be an access point card (col.13, lines 49-64 and col.14, lines 15-55). The access point establishes a channel in order to allow communication or connection amongst nodes, systems, or networks. Thus, the frequency or link is also interpreted and given as a channel that the access point interconnects the card and allows connection to devices which suggests a channel is determined if the access point has been determined corresponding to the card which permits communication amongst the network (col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53).

The claimed process associated with a node can broadly be given as a function for communication, routing, connection, session, etc. which usually includes packets or messages of information regarding the communication (col.12, lines 41-50 and col.21, lines 15-26). Shuen discloses a node is also referred as a host or mobile host (col.13, lines 50-52) and the claimed

administrative machine as a home router. Shuen explains the request (col.23, lines 36-47 and col.25, lines 14-35) to verify a first node identification associated with the first process involves the mobile host exchanges information with the home router to respond to the mobile host. The exchanged information is a local address comprising local network number and a local node number that corresponds to the local network number that may be obtained from the router which is valid (col.16, lines 41-55 and col.22, lines 62-65). The constant address corresponding to a virtual network and virtual node number created by the home router and uniquely identifying the mobile host throughout a session (col.7, lines 54-57). This information reads on the claimed first node identification associated with the first process. The constant address is the claimed virtual address where a constant address identifies a mobile host. Since the constant address is referenced to a virtual network number, it is called a virtual address (col.9, lines 11-15 and col.13, lines 7-8 and 42-48). The virtual network number and virtual node number are included in the virtual address (col.16, lines 62-67). The claimed without passing through the administrative machine obviously suggests the mobile host directly communicating with another node and not to the router (col.19, lines 13-15). Shuen discloses a mobile host may use its constant address to initiate sessions with a correspondent host (col.18, lines 60-65 and col.22, lines 13-15) and a sequenced packet exchange is an exchange of information according to a protocol by which two nodes may communicate across the network (col.30 , lines 24-34). Shuen obviously suggests a first process transmit a packet to the second process through the open socket. However, Shuen did not clearly explain transmitting a packet from the first process to the second process through the open socket without passing through the administrative machine.

Mattaway discloses the first processing unit 12 is the claimed first node and the second processing unit as the claimed second node. The claimed administrative machine can broadly be given as a server. Whether it is the connection server or mail server (col.8, line 65 – col.9, line 13 and col.12, lines 21-24), Mattaway's invention is for the first processing unit to establish direct communication links to the second processing unit without interacting or going through any server (col.9, lines 52-57 and col.26, lines 18-25). Mattaway discloses uses the server (col.7, lines 9-20) to verify a first node identification associated with the first process (col.3, lines 7-10 and col.18, lines 21-25). Mattaway discloses receiving security context information at the first node from the administrative machine, the security context information comprising a virtual address for the first node (col.7, lines 24-28 and col.18, lines 33-36) and appending the security context information for the first process in a process table (col.18, lines 21-36 and col.20, lines 15-23). A process table obviously is for comparison and matching purposes to verify or validate the received data in the packet (col.18, lines 30-36). The packet comprising the security context information for the first process in the process table (col.22, lines 21-26). Mattaway discloses point-to-point Internet communication of transmitting a packet from the first process to the second process (col.8, lines 28-29) through the open socket without processing by a server (col.8, line 65 – col.9, line 13). The only purpose is for directory and information related services (col.12, lines 36-41 and col.17, lines 17-18). Thus, Mattaway suggests direct communication link between the first process and the second process without passing through a server (col.9, lines 52-57 and col.26, lines 18-25).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Shuen to teach transmitting a packet from the first process to the second process through the open socket (Mattaway on col.8, lines 28-29) without passing through the administrative machine

(Mattaway on col.8, line 65 – col.9, line 13) because using a connection server (administrative machine) is for directory and information related services only and to verify a node so that the node can directly communicate with another node (Mattaway on col.12, lines 15-16 and 36-41 and col.26, lines 18-25).

As per claims 17 and 34: See Shuen on col.23, lines 5-30 and col.18, lines 45-55; discusses the method of claim 16, wherein obtaining a node identification further comprises: modifying a socket structure in the socket so that the socket structure accepts the node identification; and modifying a process table so that the table comprises a node identification field.

As per claim 29:

Shuen teaches a system for placing a process executed in a node in a security context, comprising:

an administrative machine; and **(col.13, lines 21-30)**

a sending node comprising:

a transmission module that transmit a request an administrative machine **(col.23, lines 36-47 and col.25, lines 14-35)** to verify a sending node identification **(col.7, lines 54-57 and col.16, lines 41-55 and col.22, lines 62-65)**, and receives security context information from the administrative machine in response to the request **(col.23, lines 60-65 and col.25, lines 14-35)**, wherein the security context information comprises a virtual address for the sending node; **(col.9, lines 11-15 and col.13, lines 7-8 and 42-48)**

memory containing a process **(col.8, lines 19-27 and col.9, lines 32-36)** and an associated process table; and **(col.18, lines 50-55 and col.23, lines 10-30)**

an appending module that appends the received security context information and the sending node identification for the process in the process table **(col.15, lines 10-35 and col.18, lines 46-49)**, wherein the transmission module transmits a packet from the process to a receiving node **(col.18, lines 13-23 and col.22, lines 13-15)** *[without passing through the administrative machine]*, the packet comprising the security context information for the first process in the process table; and **(col.12, lines 64-67 and col.13, lines 1-13)**

means for accepting the transmitted packet **(col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53)** when the first and second process belong to the channel. **(col.13, lines 49-64 and col.14, lines 40-55)**

Shuen discloses networks may include lines connecting to various nodes and an access point includes a transmitter and receiver operating at some electromagnetic frequency. Corresponding to an access point may be an access point card (col.13, lines 49-64 and col.14, lines 15-55). The access point establishes a channel in order to allow communication or connection amongst nodes, systems, or networks. Thus, the frequency or link is also interpreted and given as a channel that the access point interconnects the card and allows connection to devices which suggests a channel is determined if the access point has been determined corresponding to the card which permits communication amongst the network (col.20, lines 45-64 and col.21, lines 35-46 and col.22, lines 43-53).

The claimed process associated with a node can broadly be given as a function for communication, routing, connection, session, etc. which usually includes packets or messages of information regarding the communication (col.12, lines 41-50 and col.21, lines 15-26). Shuen discloses a node is also referred as a host or mobile host (col.13, lines 50-52) and the claimed

administrative machine as a home router. Shuen explains the request (col.23, lines 36-47 and col.25, lines 14-35) to verify a first node identification associated with the first process involves the mobile host exchanges information with the home router to respond to the mobile host. The exchanged information is a local address comprising local network number and a local node number that corresponds to the local network number that may be obtained from the router which is valid (col.16, lines 41-55 and col.22, lines 62-65). The constant address corresponding to a virtual network and virtual node number created by the home router and uniquely identifying the mobile host throughout a session (col.7, lines 54-57). This information reads on the claimed first node identification associated with the first process. The constant address is the claimed virtual address where a constant address identifies a mobile host. Since the constant address is referenced to a virtual network number, it is called a virtual address (col.9, lines 11-15 and col.13, lines 7-8 and 42-48). The virtual network number and virtual node number are included in the virtual address (col.16, lines 62-67). The claimed without passing through the administrative machine obviously suggests the mobile host directly communicating with another node and not to the router (col.19, lines 13-15). Shuen discloses a mobile host may use its constant address to initiate sessions with a correspondent host (col.18, lines 60-65 and col.22, lines 13-15) and a sequenced packet exchange is an exchange of information according to a protocol by which two nodes may communicate across the network (col.30 , lines 24-34). Shuen obviously suggests a first process transmit a packet to the second process through the open socket. However, Shuen did not clearly explain transmitting a packet from the first process to the second process through the open socket without passing through the administrative machine.

Mattaway discloses the first processing unit 12 is the claimed first node and the second processing unit as the claimed second node. The claimed administrative machine can broadly be given as a server. Whether it is the connection server or mail server (col.8, line 65 – col.9, line 13 and col.12, lines 21-24), Mattaway's invention is for the first processing unit to establish direct communication links to the second processing unit without interacting or going through any server (col.9, lines 52-57 and col.26, lines 18-25). Mattaway discloses uses the server (col.7, lines 9-20) to verify a first node identification associated with the first process (col.3, lines 7-10 and col.18, lines 21-25). Mattaway discloses receiving security context information at the first node from the administrative machine, the security context information comprising a virtual address for the first node (col.7, lines 24-28 and col.18, lines 33-36) and appending the security context information for the first process in a process table (col.18, lines 21-36 and col.20, lines 15-23). A process table obviously is for comparison and matching purposes to verify or validate the received data in the packet (col.18, lines 30-36). The packet comprising the security context information for the first process in the process table (col.22, lines 21-26). Mattaway discloses point-to-point Internet communication of transmitting a packet from the first process to the second process (col.8, lines 28-29) through the open socket without processing by a server (col.8, line 65 – col.9, line 13). The only purpose is for directory and information related services (col.12, lines 36-41 and col.17, lines 17-18). Thus, Mattaway suggests direct communication link between the first process and the second process without passing through a server (col.9, lines 52-57 and col.26, lines 18-25).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Shuen to teach transmitting a packet from the first process to the second process through the open socket (Mattaway on col.8, lines 28-29) without passing through the administrative machine

(Mattaway on col.8, line 65 – col.9, line 13) because using a connection server (administrative machine) is for directory and information related services only and to verify a node so that the node can directly communicate with another node (Mattaway on col.12, lines 15-16 and 36-41 and col.26, lines 18-25).

As per claim 30: See Shuen on col.7, lines 54-57 and col.16, lines 41-55 and col.22, lines 62-65; discusses the transmission module further receives a key that corresponds to the sending node identification from the administrative machine.

As per claim 31: See Shuen on col.15, lines 10-35 and Mattaway on col.26, lines 46-50; discusses discussing an encryption module that encrypts the packet transmitted by the process using the key; and an encapsulating module that encapsulates the encrypted packet with a header that comprises the sending node identification.

As per claim 44: See Shuen on col.16, lines 41-55 and col.18, lines 46-49and col.22, lines 10-14 and 62-65; discusses the computer readable medium of claim 35, wherein the appending module comprises: an obtaining module for obtaining the security context information from a third process, the security context comprising a virtual address and a node identification; and a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification.

As per claims 46-48: Cancelled

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435